UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**No.** 2:24-mj-515
	)	
The person of Kevin Michael Ireland, DOB: 4/14/88;	)	
the residence located at 2750 Hilliard Rome Road,	)	**Magistrate Judge:**
Hilliard, Ohio 43026, including any curtilage, detached	)	
buildings and garages, and any computers or digital	)	
media located therein/thereon associated to Kevin Ireland	)	**UNDER SEAL**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

I, Amanda North (Your Affiant), a Special Agent with the Ohio Bureau of Criminal Investigation (BCI) and assigned as a Task Force Officer (TFO) for the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent (SA) with BCI, since 2022, and have been in the Special Victims Unit since 2013, where I was previously a Criminal Investigator. I have been a TFO at the FBI Columbus Resident Agency since early 2023. I am primarily responsible for investigating child sexual exploitation and internet crimes, as well as hands on offenses of abuse involving juveniles and the elderly.
2. During my career as a Criminal Investigator, I have received more than one hundred hours of training in internet investigations, to include Peer to Peer software. I was assigned full-time to the Franklin County Internet Crimes Against Children Task Force (ICAC), from January of 2016 through my promotion to SA in May of 2022. I was also a TFO for Homeland Security from 2018 until the end of 2021, when I was designated to be assigned to the FBI VCAC Unit. I have participated in various investigations of child exploitation and have executed numerous search warrants, interviews and arrests that resulted in conviction. As part of my duties as a TFO, I investigate criminal violations relating to child exploitation and child pornography violations, including the illegal production, distribution, transmission,

receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

3. As a TFO with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFDAVIT

4. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the locations specifically described in **Attachments A, B, and C** of this Affidavit. The facts and statements set forth in this affidavit are based on my knowledge, experience, and investigation, as well as the knowledge, experience, and investigative findings of others with whom I have had communications about this investigation, including other law enforcement officers and agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause for a search warrant for the person of Kevin Michael Ireland, DOB 4/14/1988 (the **SUBJECT PERSON**) and the residence located at 2750 Hilliard Rome Road, Hilliard, Ohio 43026 (the **SUBJECT PREMISES**). I have not omitted any facts that would negate probable cause.

5. The **SUBJECT PERSON** and **SUBJECT PREMISES** to be searched are more particularly described in **Attachment A** and **Attachment B** respectively, for the items specified in **Attachment C,** which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A – sexual exploitation of a minor, advertising/solicitation for/or, and distribution and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter "child pornography"), distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the **SUBJECT PERSON** and the entire **SUBJECT PREMISES**, including the residential dwelling, curtilage, detached buildings and storage units, for any computers, cellular "smart" phones and/or mobile computing device or digital media located thereon/therein, and to thereafter seize and examine any such device that is recovered from the **SUBJECT PERSON** or **SUBJECT PREMISES**, for items specified in **Attachment C**,

and to seize all items listed in **Attachment C** as evidence, fruits, and instrumentalities of the above violations.

APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.
7. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.
8. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.

9. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.
10. As it is used in 18 U.S.C. §§ 2251 and 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2)(A) as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.
11. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography"[1] is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.
12. The term "sexually explicit conduct" has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i)

[1] The term child pornography is used throughout this affidavit. All references to this term in this affidavit and Attachments A and B hereto, include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. §§ 2251 and 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

13. The term "minor", as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1) as "any person under the age of eighteen years."
14. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."
15. The term "visual depiction," as used herein, is defined pursuant to T18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."
16. The term "computer" is defined in 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.
17. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).
18. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which

records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

19. Internet Service Providers" (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

20. "Internet Protocol address" (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

21. As it is used throughout this affidavit and all attachments hereto, the term "storage media" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

BACKGROUND REGARDING THE INTERNET AND MOBILE APPLICATIONS

22. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

23. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.

24. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including "GIF" (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

25. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

26. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 128GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 16 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via

the tablet. Modern cell phones have average storage capabilities ranging from 32 Gigabytes to 256 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

27. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet

Protocol ("IP") addresses and other information both in computer data format and in written record format.

28. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography, or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

29. It is often possible to recover digital or electronic files, or remnants of such files, months or sometimes even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

30. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

31. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.
32. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in **Attachment C**.
33. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include KIK messenger service, Snapchat, X (formerly known as Twitter), and Instagram.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

34. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:
    - Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information.

Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

- Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

35. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

36. In addition, there is probable cause to believe that any computer or mobile computing device and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251, 2252, 2252A should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

37. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in **Attachment C;**
- Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in **Attachment C;**
- Surveying various files, directories and the individual files they contain;
- Opening files in order to determine their contents;
- Scanning storage areas;
- Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or
- Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment C**.

INVESTIGATION AND PROBABLE CAUSE

38. On or about September 17, 2024, the FBI's Columbus Child Exploitation and Human Trafficking Task Force (CEHTTF) received an email from the Jackson County Sheriff's Office. The email contained information about a Child Victim Identification Program (CVIP) image analysis report from the National Center for Missing and Exploited Children (NCMEC). The CVIP is a component of the FBI and is designed to help identify the victims of child exploitation offenses. More specifically, the CVIP report stated that while the NCMEC was reviewing CyberTipline Report #133900266 and its associated media which had been submitted to them by Google on or about September 7, 2022, two images of apparent child sexual exploitation of a prepubescent female child were depicted on the media. The images were flagged because they had been in the NCMEC database, but the CVIP report noted that to date, no one had been able to identify the minor female in the images or the individual who produced them.

39. Both images, titled "*20150417_114910.jpg*" and "*20150417_114938.jpg*" respectively, depicted a prepubescent female child seen spreading apart her genitalia to the camera with the focus being the close-up image of her nude vagina with two fingers right above it.

40. Based on training and experience with the NCMEC, your affiant knows that in any investigation related to a child exploitation target, image and video files recovered from the digital media devices that is suspected or known to be child pornography is submitted to the NCMEC. The NCMEC then cross references those files to see if the minor child in them has been previously identified. Based on your affiants understanding of the NCMEC process, the files are then saved in this repository in case they resurface again in another investigation which is what happened here when they were uploaded to the Google Photo infrastructure in November 2022. The two images outlined above were in the NCMEC database – meaning at some point, they had been submitted to the NCMEC for review – and the two images were given a series name and remained in the NCMEC repository of child exploitation material. At the time of this upload on September 7, 2022, NCMEC flagged the photos as previously having been in their database but with no victim yet identified in the content.
41. The CyberTipline Report had indicated that two images of child pornography had been uploaded to Google Photos infrastructure by Google email address kevinire025@gmail.com. The CyberTipline Report also identified the name on the account as Kevin **IRELAND. IRELAND** reported date of birth as April 14, 1988 and verified telephone phone number as (740) 505-6956. IP address login information was also provided.
42. Metadata for the two files was provided and listed the following information:

Make:	LG Electronics
Model:	LG-D850
CreateDate:	2015-04-17 11:49:38
GPS Latitude:	38.898818944444443
GPS Longitude:	-82.5727005

43. The NCMEC report indicated that the GPS coordinates related to the metadata for the two flagged images resolved to the address of 229 Aetna Street, Oak Hill, Ohio 45656. A preliminary search of that address by the NCMEC using law enforcement databases revealed that between March 2015 and January 2017, Kevin M. **IRELAND**, with a date of birth of 4/14/1988, had resided at the residence at that address. Because the NCMEC had not been previously able to identify the minor victim depicted in the content, they sent the lead to Ohio in order to further investigative after obtaining the above noted metadata.
44. In addition to the two images outlined above, **IRELAND's** Google account also uploaded two more files of child sexual abuse material. The file titled "*0108121823a.jpg*" depicted

an adult male penis next to the mouth of an infant child. The file titled "*video-av_nyuu_info-16497023525895.mp4*" contained an approximately 10 minute and 21 second video which depicted a minor female, approximately nine to twelve years of age, undressing herself and displaying her vagina as well as masturbating.

45. In addition to the CyberTipline Report noted above, three additional NCMEC CyberTipline reports were linked to **IRELAND** by the same name, phone number, date of birth, and email address provided in the initial CyberTipLine Report. These reports had been submitted to the NCMEC by Google, LLC and involved the upload of child pornography to the Google Photo infrastructure. The reports were broken down as followed:

    - CyberTipline Report #133924823 was submitted by Google, LLC on or about September 8, 2022, and contained one file, titled "*VID_20210708_133143_340.mp4*". The file, which was an video approximately 20 seconds in length, depicted a young prepubescent minor female, approximately six to nine years of age, nude from the waist down. In the video, the prepubescent female was bent over on her hands and knees while an adult male penetrated her vagina with his penis from behind.

    - CyberTipline Report #136009850 was submitted by Google, LLC on or about October 5, 2022, and contained one file, titled, "*20150303_201655.jpg*" which depicted a toddler, between one to three years of age, fully nude and laying face down on a blanket facing away from the camera.

    - CyberTipline Report #136061566 was submitted by Google, LLC on or about October 6, 2022, and contained one file, titled "*2022-08-14_13-03-13.mp4*" and contained a video approximately 52 seconds in length which depicted a screen recording of a cell phone scrolling through different folders which appeared to contain child sexual abuse material.

46. In September 2024, after law enforcement received the reports and above information, they began to investigate where **IRELAND** was residing and whether he lived in the Southern District of Ohio. In doing so, an OHLEG search of for **IRELAND** with a DOB of 4/14/1988 identified Kevin Michael **IRELAND** as residing at an address of 222 Sullivan Avenue, in London, Ohio 43140. Further open-source social media checks revealed that he was in a relationship with a female, M.L., whose residence was also listed in London, Ohio.

47. On September 20, 2024 and September 26, 2024, surveillance was conducted at the residence of 222 Sullivan Avenue. No vehicles were located at the Sullivan Avenue address and **IRELAND** was not seen in the area. Your affiant made contact with local law enforcement, who advised that a recent call for service to the Sullivan Avenue residence resulted in them

identifying who lived at the residence and per that report and the officers who took it, **IRELAND** had not resided at the Sullivan Avenue location for months.

48. Additional checks on any vehicle that could be registered to **IRELAND** was completed and law enforcement learned he had no vehicles registered to his name. A check into M.L. revealed that Ohio license plate JVK8287 was registered to her.

49. Flock footage, which is a license plate reading camera system and video/photo database, identified Ohio license plate JVK8287 as driving around the Hilliard, Ohio area. Flock also provided some images from the license plate reads and in those images, **IRELAND** was depicted as sitting in the front passenger seat on a black Town & Country vehicle with that license plate attached.

50. On or about October 21, 2024, law enforcement learned that FCCS had responded to the address of 2750 Hilliard Rome Road in Hilliard, Ohio (the **SUBJECT PREMISES**) on an unrelated incident. Your affiant then spoke with the FCCS case workers who informed your affiant that they had just been inside the **SUBJECT PREMISES** and that **IRELAND** was inside and had represented to them that he lived there. Your affiant also learned that five minor female children between the ages of nine and twelve also resided at the **SUBJECT PREMISES**.

51. Hilliard Police Department (HPD) also confirmed that **IRELAND** resided at the **SUBJECT PREMISES** and worked at White Castle. Your affiant learned through further investigation that M.L. drives **IRELAND** to work which is consistent with him being see in the front passenger seat of her vehicle in the Hilliard, Ohio area.

COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

52. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in communicating about and engaging in sexual abuse of children:

- Those who communicate about and engage in sexual abuse of children and exchange or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing

children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.

- Those who communicate about and engage in sexual abuse of children and trade or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- Those who communicate about and engage in sexual abuse of children and trade or collect child pornography sometimes maintain any "hard copies" of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections and communications are often maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.
- Those who communicate about and engage in sexual abuse of children and trade or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

- When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

53. Based upon the conduct of individuals involved in creating, uploading, receiving, distributing, and/or collecting child pornography set forth in the above paragraphs, and the facts learned during the investigation in this case, namely, that Kevin **IRELAND,** an individual residing at the **SUBJECT PREMISES,** was engaged in the uploading of child pornography to a Google Photos account associated with his name. Specifically, **IRELAND** uploaded images and videos of child pornography and two images which were flagged by the NCMEC has having been newly created content. Therefore, your affiant has reason to believe that **IRELAND** has a sexual interest in minors and has created, viewed, or sought out visual depictions of minors engaged in sexually explicit conduct utilizing an internet-capable device. Your affiant therefore submits that there is probable cause to believe the evidence of the offenses of 18 U.S.C. §§ 2251, 2252, and 2252A – sexual exploitation of a minor, advertising/solicitation for/or, and distribution and receipt of visual depictions of minors engaged in sexually explicit conduct (hereinafter "child pornography"), distribution, transmission, receipt, and/or possession of child pornography, will be located on the **SUBJECT PERSON** and/or in the **SUBJECT PREMISES** and any digital device associated to Ireland that may be found on/in the **SUBJECT PERSON** or the **SUBJECT PREMISES.**

CONCLUSION

54. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of Title 18, United States Code, Sections 2251, 2252, and 2252A have been committed, and evidence of those violations is located on the person described in **Attachment A** and in the residence described in **Attachment B**. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in **Attachment C**.

Amanda North #118

Amanda North
TFO
Federal Bureau of Investigation

Sworn to and subscribed before me this 25th day of October, 2024.

Chelsey M. Vascura

Chelsey M. Vascura
United States Magistrate Judge
United States District Court
Southern District of Ohio